UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Apple Inc. iCloud Account:
gustavsstern@gmail.com,
more fully described in Attachment A

Case No. 3:23-mj-05372

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Apple iCloud Account, more fully described in Attachment A, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1801(a)	Video Voyeurism

The application is based on these facts:

✓ See Affidavit of OSI Special Agent Tyler Creasey-Parks, attached hereto and incorporatated herein by reference.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

CREASEYPARKS.TYLER.RAY.1393364366 Digitally signed by CREASEYPARKS.TYLER.RAY.1393364366 Date: 2023.10.18 13:51:48 -07'00'

Applicant's signature

TYLER R. CREASEY-PARKS, Special Agent, OSI

Printed name and title

◉ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 10/19/2023

Judge's signature

City and state: Tacoma, Washington

THERESA L. FRICKE, United States Magistrate Judge

Printed name and title

AFFIDAVIT OF SPECIAL AGENT TYLER R. CREASEY-PARKS

STATE OF WASHINGTON)
)
COUNTY OF PIERCE)

I, Tyler R. Creasey-Parks, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with an iCloud account that [is/are] stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent (SA) of the Department of the Air Force Office of Special Investigations (OSI) and have been employed by the OSI since 4 Mar 22. I am currently detailed to the OSI Detachment 305, Joint Base Lewis-McChord (JBLM), Washington. As a SA, I have completed the Criminal Investigator Training Program (CITP) and Basic Special Investigations Course (BSIC) at Federal Law Enforcement Training Facility (FLETC) located in Glynco, Georgia. These courses included legal classes, investigative techniques, evidence preservation and collection, financial related crimes, and computer related crimes. I have received additional

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

training and certifications in Sex Crimes Investigators Training Program (SCITP). As a SA in OSI, I am authorized to investigate violations of the Uniform Code of Military Justice (UCMJ) and applicable Federal and State laws where there is a Military Nexus. Through the course of my employment in law enforcement, I have led and assisted in numerous different investigations including but not limited to sexual abuse, domestic violent extremism (DVE), and Illegal Substance use and Distribution.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1801(a) (Video Voyeurism) have been committed by GUSTAV STERN. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

SUMMARY OF PROBABLE CAUSE

5. I am a Special Agent assigned to an ongoing OSI investigation of GUSTAV STERN, herein referred to as STERN**,** suspected of video voyeurism of his wife, herein referred to as "SS". The following sets forth the facts and circumstances for the search and seizure:

a. On 20 Jun 22, SS was on her and STERN's shared MacBook computer and received an email notification, addressed to STERN, for a KeepSafe account verification. SS conducted a google search of KeepSafe application, which indicated it was an application to safeguard images and videos. Following the google search, SS viewed the images and videos on the shared iCloud account, which was under email address: Gustavsstern@gmail.com and located multiple nude images of SS and approximately three or four videos of STERN and SS having sexual intercourse in the deleted folder. SS

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

clarified she never sent STERN nude images of herself and never consented to being recorded.

b. SS stated all videos took place in their bedroom. SS recalled in one video she was faced down with her buttocks shown and a pink vibrator sex toy was used. In another video, STERN placed his hands on SS's vagina. SS disclosed she identified herself in the video by a skin tag on her inner left thigh and she identified STERN by a tattoo on one of his middle fingers. Furthermore, SS was unaware when or how STERN took the videos and images since she had been accustomed to STERN using his flashlight on his phone and she was not sure if he had recorded or used his flashlight. SS did not know where STERN placed his phone to record or photograph her.

c. After SS located the nude videos and images of herself, she immediately called STERN, recorded the telephonic conversation, and confronted him about the images and videos. During the phone call, STERN admitted to being wrong for having the images and videos and disclosed he kept them because SS wanted to divorce him and he did not want to lose them. Following the confrontation, SS was no longer able to access the photos and videos and believed STERN changed the passwords to his iCloud account.

d. On May 9, 2023, agents interviewed, James O'Kelly, First Sergeant, 22 STS, JBLM, WA, who disclosed on approximately 27 April 2023, STERN informed First Sergeant O'Kelly both SS and he had nude photographs of each other they exchanged throughout their marriage.

//

//

//

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

BACKGROUND CONCERNING APPLE[1]

7. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

8. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations,

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

9. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

(including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

10. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

11. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

12. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

13. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple. In my training and experience, evidence of STERN using Apple ID under gustavsstern@gmail.com and/or DSID: 8017086620, had evidence

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

related to criminal activity of the kind described above, which may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the Department of the Air Force to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

14. For example, the stored files connected to Apple ID under gustavsstern@gmail.com and/or DSID: 8017086620 may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

15. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

16. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g.,

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

17. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning STERN and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

18. Based on the information set forth herein, I submit that this affidavit supports probable cause for a warrant to search the iCloud account as described in Attachment A, for evidence and instrumentalities, as described in Attachment B, of the crimes of Video Voyeurism, in violation of 18 U.S.C. § 1801(a).

CREASEYPARKS.TYLER.RAY.1393364366 Digitally signed by CREASEYPARKS.TYLER.RAY.1393364366 Date: 2023.10.18 13:52:09 -07'00'

TYLER R. CREASEY-PARKS
Special Agent, OSI Detachment 305

The above-name agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on this 19th day of October, 2023.

Theresa L. Fricke

The Honorable Theresa L. Fricke
United States Magistrate Judge

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following iCloud Account that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California:

Name: Gustav Samuel Stern

Email: gustavsstern@gmail.com

Phone Number: 661-388-1971

DSID: 8017086620

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

ATTACHMENT B

Items to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

1. To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on 11 August 2023, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"),

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. All photos and videos stored on iCloud from 1 June 2022 to 18 April 2023, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Photo Sharing, My Photo Stream, and iCloud Photo Library, and all images, videos.

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1801(a) (Video Voyeurism), those violations involving GUSTAV STERN and occurring after 1 June 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Photographs and videos which may contain explicit images of SS, stored on GUSTAV STERN'S iCloud account from 1 June 2022 to 18 April 2023.

b. Evidence indicating how and when the photographs or videos were taken, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

This warrant authorizes a review of electronic media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, ad technical experts. Pursuant to this warrant, the OSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

THE SEIZURE OF ELECTRONIC MEDIA SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH ELECTRONIC MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800